



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,721	01/18/2001	Mitsuru Maeda	35.C15052	5429

5514 7590 11/23/2004

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER

BAUM, RONALD

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 11/23/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/761,721

Applicant(s)

MAEDA, MITSURU

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 6 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-42 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08).
Paper No(s)/Mail Date <u>4</u> . | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

1. Claims 1-42 are pending for examination.
2. Claims 1-42 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 10 recites the limitation "An apparatus according to *claim 8*, ... result of *said authentication means*.". There is insufficient antecedent basis for this limitation in the claim.

The examiner assumes for the sake of applying art that the "claim 8" should be "claim 9".

Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 11 recites the limitation "An apparatus according to *claim 1*, ...". The examiner assumes for the sake of applying art that the "*claim 1*" should be "*claim 8*".

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-4,6-12,17-21,23-29,34-42 are rejected under 35 U.S.C. 102(b) as being anticipated by Kim et al, U.S. Patent 5,799,081.

5. As per claim 1; "An information processing apparatus [figure 4 and accompanying descriptions, whereas the illegal view/copy protection apparatus as broadly interpreted by the examiner would clearly encompass 'An information processing apparatus'.] comprising: a) input means for inputting information data [figures 4,5,6,8,9,10-12,16 and accompanying descriptions, whereas the illegal view/copy protection apparatus content information input, as broadly interpreted by the examiner would clearly encompass '... inputting ... data'.]; b) generation means for generating security data to be used to protect the information data [figures 4,5,6,8,9,10-12,16 and accompanying descriptions, whereas the illegal view/copy protection apparatus CPTC information, as broadly interpreted by the examiner would clearly encompass '... security data ... protect ... data'.]; c) encoding means for encoding the information data to generate encoded data [figures 4,6,8,10-12,16 and accompanying descriptions, whereas the illegal view/copy protection apparatus MPEG encoding/decoding components, as broadly interpreted by the examiner would clearly encompass '... generate encoded data'.]; d) extraction means for extracting a unique predetermined code indicating a specific meaning from encoded data within a security section in accordance with the security data [figures 4,6,9-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data multiplexing and combining, as broadly interpreted by the examiner would clearly encompass '... extracting ... code ... encoded data ... accordance with the security data'.]; e) superimposing means for superimposing the security data on the predetermined code [figures 4,6,9-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data multiplexing and combining, as broadly interpreted by the examiner would clearly encompass '... superimposing the security data ... code'.]; f) scrambling means for scrambling the encoded

Art Unit: 2136

data except for the predetermined code within the security section [figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data scrambling / multiplexing and combining, as broadly interpreted by the examiner would clearly encompass '... scrambling means ...'.]; and g) output means for outputting the predetermined code processed by said superimposing means and the encoded data processed by said scrambling means [figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus functional output elements, as broadly interpreted by the examiner would clearly encompass 'output means ...'.].";

Further, as per claim 18; "An information processing method [This claim is the method claim for the apparatus claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] comprising the steps of: a) inputting information data; b) generating security data to be used to protect the information data; c) encoding the information data to generate encoded data; d) extracting a unique predetermined code indicating a specific meaning from encoded data within a security section in accordance with the security data; e) superimposing the security data on the predetermined code; f) scrambling the encoded data except for the predetermined code within the security section; and g) outputting the superimposed predetermined code and the scrambled encoded data.";

Further, as per claim 39; "A computer readable storage medium [This claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] which stores a control program that implements an image processing method cited in claim 18."

6. Claim 2 ***additionally recites*** the limitation that; “An apparatus according to claim 1, wherein the security data contains key information to be used by said scrambling means.”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data scrambling / multiplexing and combining associated control word(s), as broadly interpreted by the examiner would clearly encompass ‘... key information ...’);

Further, as per claim 19 ***additionally reciting*** the limitation that; “A method [This claim is the method claim for the apparatus claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection] according to claim 18, wherein the security data contains key information to be used in said scrambling step.”.

7. Claim 3 ***additionally recites*** the limitation that; “An apparatus according to claim 1, wherein the security data contains information for an authentication process.”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data scrambling / multiplexing and combining associated CPTC and control word(s), and more particularly, the CA smart card elements and software, as broadly interpreted by the examiner would clearly encompass ‘... authentication process’);

Further, as per claim 20 ***additionally reciting*** the limitation that; “A method [This claim is the method claim for the apparatus claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection] according to claim 18, wherein the security data contains information for an authentication process.”.

8. Claim 4 ***additionally recites*** the limitation that; “An apparatus according to claim 1, wherein the information data is image data, and said encoding means generates an MPEG-4 bitstream.”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4,6,8,10-12,16 and accompanying descriptions, whereas the illegal view/copy protection apparatus MPEG encoding/decoding components used for video/audio data streams, as broadly interpreted by the examiner would clearly encompass ‘...image data, ... MPEG-4’.);

Further, as per claim 21 ***additionally reciting*** the limitation that; “A method [This claim is the method claim for the apparatus claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection] according to claim 18, wherein said encoding step includes a step of generating an MPEG-4 bitstream.”.

9. Claim 6 ***additionally recites*** the limitation that; “An apparatus according to claim 1, further comprising enciphering means for enciphering the security data, and wherein said superimposing means superimposes the security data enciphered by said enciphering means.”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data scrambling (encryption) / descrambling (decryption), as broadly interpreted by the examiner would clearly encompass ‘... enciphering means ...’.);

Further, as per claim 23 ***additionally reciting*** the limitation that; “ A method [This claim is the method claim for the apparatus claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection] according to claim 18, further comprising an enciphering step

Art Unit: 2136

of enciphering the security data, and wherein said superimposing step includes a step of superimposing the security data enciphered in said enciphering step.”.

10. Claim 7 *additionally recites* the limitation that; “An apparatus according to claim 1, wherein the predetermined code to be extracted by said extraction means is a start code. ”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4,6,9-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data CPTC information, as associated with the multiplexing and combining data stream protocol assembly aspects insofar as the protocol clearly deals with “where” the fields of data will be assembled into the said data stream (i.e., the start or “start code” designated positioning), as broadly interpreted by the examiner would clearly encompass ‘...extracting ... start code’.);

Further, as per claim 24 *additionally reciting* the limitation that; “A method [This claim is the method claim for the apparatus claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection] according to claim 18, wherein the predetermined code to be extracted in said extraction step is a start code.”.

11. As per claim 8; “An information processing apparatus [This claim is the ‘receiving (i.e., sink) side’ apparatus claim for the ‘transmitting (i.e., source) side’ apparatus claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection (i.e., figures 4,6,9-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus clearly is a source and sink for the processed data content.))] comprising: a) input means for inputting encoded data in which security data is adaptively superimposed on a unique predetermined code

Art Unit: 2136

in the encoded data, which indicates a specific meaning, and the encoded data except for the predetermined code is adaptively scrambled in accordance with the security data; b) code extraction means for extracting from the encoded data a code which is located at a position where the predetermined code is present; c) detection means for detecting the security data from the extracted code; d) descrambling means for descrambling the encoded data in accordance with a detection result of said detection means; and e) decoding means for decoding image encoded data descrambled by said descrambling means.”;

Further, as per claim 25; “An information processing method [This claim is the method claim for the apparatus claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection] comprising the steps of: a) inputting encoded data in which security data is adaptively superimposed on a unique predetermined code in the encoded data, which indicates a specific meaning, and the encoded data except for the predetermined code is adaptively scrambled in accordance with the security data; b) extracting from the encoded data a code which is located at a position where the predetermined code is present; c) detecting the security data from the extracted code; d) descrambling the encoded data in accordance with the detection result; and e) decoding the descrambled image encoded data.”;

Further, as per claim 40; “A computer readable storage medium which stores a control program [This claim is the embodied software claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection] that implements an image processing method cited in claim 25.”.

Art Unit: 2136

12. Claim 9 *additionally recites* the limitation that; "An apparatus according to claim 8, wherein the security data contains authentication data to be used to check authenticity, and said apparatus further comprises authentication means for checking authenticity.". The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data scrambling / multiplexing and combining associated CPTC and control word(s), and more particularly, the CA smart card elements and software, as broadly interpreted by the examiner would clearly encompass '... authentication means for checking authenticity'.);

Further, as per claim 26 *additionally reciting* the limitation that; "A method [This claim is the method claim for the apparatus claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection] according to claim 25, wherein the security data contains authentication data to be used to check authenticity, and said method further comprises an authentication step of checking authenticity.".

13. Claim 10 *additionally recites* the limitation that; "An apparatus according to claim 8, wherein said descrambling means descrambles scrambled encoded data in accordance with a checking result of said authentication means.". The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus clearly can only descramble if the CA aspects (i.e., authentication via the smart card) enable the apparatus operation, as broadly interpreted by the examiner would clearly encompass '... checking result of said authentication means ...'.);

Further, as per claim 27 *additionally reciting* the limitation that; “A method [This claim is the method claim for the apparatus claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection] according to claim 26, wherein said descrambling step includes a step of descrambling scrambled encoded data in accordance with a checking result in said authentication step.”.

14. Claim 11 *additionally recites* the limitation that; “An apparatus according to claim 1, wherein the security data is enciphered data, and said apparatus further comprises deciphering means for deciphering the enciphered security data.”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data scrambling (encryption) / descrambling (decryption), as broadly interpreted by the examiner would clearly encompass ‘... deciphering the enciphered ...’.);

Further, as per claim 28 *additionally reciting* the limitation that; “A method [This claim is the method claim for the apparatus claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection] according to claim 25, wherein the security data is enciphered data, and said method further comprises a deciphering step of deciphering the enciphered security data.”.

15. Claim 12 *additionally recites* the limitation that; “An apparatus according to claim 8, wherein the encoded data is MPEG-4 bitstream data.”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4,6,8,10-12,16 and accompanying descriptions, whereas

Art Unit: 2136

the illegal view/copy protection apparatus MPEG encoding/decoding components used for video/audio data streams, as broadly interpreted by the examiner would clearly encompass '... MPEG-4 ...');

Further, as per claim 29 *additionally reciting* the limitation that; "A method [This claim is the method claim for the apparatus claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection] according to claim 25, wherein the encoded data is MPEG-4 bitstream data."

16. Claim 17 *additionally recites* the limitation that; "An apparatus according to claim 8, wherein the predetermined code is a start code." The teachings of Kim et al are directed towards such limitations (i.e., figures 4,6,9-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data CPTC information, as associated with the multiplexing and combining data stream protocol assembly aspects insofar as the protocol clearly deals with "where" the fields of data will be assembled into the said data stream (i.e., the start or "start code" designated positioning), as broadly interpreted by the examiner would clearly encompass '... start code');

Further, as per claim 34 *additionally reciting* the limitation that; "A method [This claim is the method claim for the apparatus claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection] according to claim 25, wherein the predetermined code is a start code."

17. As per claim 35; “An information processing method [This claim is the combination of claims 8,21 above, and is rejected for the same reasons provided for the claims 8,21 rejections, whereas the MPEG coding inherently involves the use of media objects, which is in itself a clearly hierarchical structure (i.e., figures 4,6,8,10-12,16 and accompanying descriptions, whereas the illegal view/copy protection apparatus MPEG encoding/decoding components used for video/audio data streams, as broadly interpreted by the examiner would clearly encompass ‘...image encoded data that forms a hierarchical structure’.)] comprising the steps of: a) inputting image encoded data that forms a hierarchical structure; b) extracting a predetermined code indicating a head of a predetermined layer from the image encoded data; and c) superimposing security data for image protection onto the predetermined code extracted in said extraction step.”;

Further, as per claim 41; “A computer readable storage medium which stores a control program [This claim is the embodied software claim for the method claim 35 above, and is rejected for the same reasons provided for the claim 35 rejection] that implements an image processing method cited in claim 35.”.

18. Claim 36 ***additionally recites*** the limitation that; “A method according to claim 35, further comprising an enciphering step of enciphering the image encoded data in accordance with the security data.”. The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus digital data scrambling (i.e., enciphering) / multiplexing and combining associated

Art Unit: 2136

control word(s), as broadly interpreted by the examiner would clearly encompass '...enciphering the image encoded data in accordance with the security data ...'.');

19. As per claim 37; "An information processing method [This claim is the 'receiving (i.e., sink) side' method claim for the 'transmitting (i.e., source) side' method claim 35 above, and is rejected for the same reasons provided for the claim 35 rejection (i.e., figures 4,6,9-16 and accompanying descriptions, whereas the illegal view/copy protection apparatus clearly is a source and sink for the processed data content.)] comprising the steps of: a) inputting encoded data in which security data is superimposed on a predetermined code indicating a head of a predetermined layer of image encoded data that forms a hierarchical structure; b) extracting from the encoded data a code which is located at a position where the predetermined code is present; c) detecting the security data from the extracted code; and d) decoding the encoded data in accordance with a detection result.";

Further, as per claim 42; "A computer readable storage medium which stores a control program [This claim is the embodied software claim for the method claim 37 above, and is rejected for the same reasons provided for the claim 37 rejection] that implements an image processing method cited in claim 37."

20. Claim 38 *additionally recites* the limitation that; "A method according to claim 37, wherein the encoded data is enciphered data, and said decoding step includes a step of deciphering the enciphered encoded data." The teachings of Kim et al are directed towards such limitations (i.e., figures 4-6,8-16 and accompanying descriptions, whereas the illegal view/copy

Art Unit: 2136

protection apparatus digital data scrambling (i.e., enciphering) / multiplexing and combining associated control word(s), and descrambling (i.e., deciphering) / demultiplexing and combining via associated control word(s), as broadly interpreted by the examiner would clearly encompass '...deciphering the enciphered encoded data ...').

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

21. Claims 5,13-16,22,30-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al, U.S. Patent 5,799,081 as applied respectively, to claims 4,12,21,29 above, and further in view of Dawson, Ken, "MPEG-4: A Bird's Eye View", Carleton University, Hello World!, Issue 2, Vol. 1, "http://www.cosc.brocku.ca/~cspress/HelloWorld/1999/04-apr/mpeg4_a_birds_eye_view.html".

As per claim 5 ***additionally reciting*** the limitation that; "An apparatus according to claim 4, further comprising IPMP encoding means for generating IPMP data indicating information that pertains to the security, and wherein said output means outputs the IPMP data generated by said IPMP encoding means.";

Further, as per claim 22 ***additionally reciting*** the limitation that; "A method [This claim is the method claim for the apparatus claim 5 above, and is rejected for the same reasons

Art Unit: 2136

provided for the claim 5 rejection] according to claim 21, further comprising an IPMP encoding step of generating IPMP data indicating information that pertains to the security, and wherein said output step includes a step of outputting the IPMP data generated in the IPMP encoding step.”.

As per claim 13 *additionally reciting* the limitation that; “An apparatus according to claim 12, wherein said input means inputs IPMP data indicating information which pertains to security.”;

Further, as per claim 30 *additionally reciting* the limitation that; “A method [This claim is the method claim for the apparatus claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection] according to claim 29, wherein said input step includes a step of inputting IPMP data indicating information which pertains to security.”.

As per claim 14 *additionally reciting* the limitation that; “An apparatus according to claim 13, wherein the IPMP data contains authentication data to be used to check authenticity, and said apparatus further comprises authentication means for checking authenticity in accordance with the authentication data.”;

Further, as per claim 31 *additionally reciting* the limitation that; “A method [This claim is the method claim for the apparatus claim 14 above, and is rejected for the same reasons provided for the claim 14 rejection] according to claim 30, wherein the IPMP data contains authentication data to be used to check authenticity, and said method further comprises an authentication step of checking authenticity in accordance with the authentication data.”.

As per claim 15 *additionally reciting* the limitation that; “An apparatus according to claim 14, wherein said descrambling means descrambles scrambled encoded data in accordance with a checking result of said authentication means.”;

Further, as per claim 32 *additionally reciting* the limitation that; “A method [This claim is the method claim for the apparatus claim 15 above, and is rejected for the same reasons provided for the claim 15 rejection] according to claim 31, wherein said descrambling step includes a step of descrambling scrambled encoded data in accordance with a checking result in said authentication step.”.

As per claim 16 *additionally reciting* the limitation that; “An apparatus according to claim 15, wherein the security data is enciphered data, and said apparatus further comprises deciphering means for deciphering the enciphered security data.”;

Further, as per claim 33 *additionally reciting* the limitation that; “A method [This claim is the method claim for the apparatus claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection] according to claim 31, wherein the security data is enciphered data, and said method further comprises a deciphering step of deciphering the enciphered security data.”.

The teachings of Kim et al suggest the base claim (“An information processing apparatus [and associated method / means / software embodiment] comprising: a) input means ... b) generation means ... c) encoding means ... d) extraction means ... e) superimposing means ... f) scrambling means ... and g) output means ... wherein the information data ... encoding means generates an MPEG-4 bitstream”, and “... authentication [dependent claims 15,16,32,33] / enciphering (encryption) / deciphering (decryption) [dependent claims 16,33] ...”) limitations

Art Unit: 2136

(figures 4,5,6,8,9,10-12,16 and accompanying descriptions) *without explicitly teaching* of the use of the various IPMP functions involved with the security generally, and authentication, more particularly, when MPEG (-4) functionality is involved.

Dawson teaches of using the IPMP system applications "Intellectual Property Rights (IPR) Protection" aspects of MPEG for rights protection via rights objects (i.e., identification, security / authentication information, etc., "Intellectual Property Rights (IPR) Protection" paragraph, pages 6-7).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Kim et al '... information processing apparatus [and associated method / means / software embodiment] comprising: ... encoding means generates an MPEG-4 bitstream', with the various IPMP functions involved with the MPEG rights protection.

Such motivation to combine would clearly encompass the need to allow secure transfer of the rights associated with the content via the MPEG encoding insofar as the whole point of having the rights protection associated with said content is so the specified security / authentication servicing related to the content is also transferred to prevent content rights violation (i.e., again, Dawson "Intellectual Property Rights (IPR) Protection" paragraph, pages 6-7).

Conclusion


Art Unit: 2136

22. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3681. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100